# 目 录

1 公钥管理 1-1
1.1 公钥管理配置命令 1-1
1.1.1 display public-key local public 1-1
1.1.2 display public-key peer 1-5
1.1.3 peer-public-key end 1-6
1.1.4 public-key local create 1-7
1.1.5 public-key local destroy 1-10
1.1.6 public-key local export dsa 1-11
1.1.7 public-key local export ecdsa 1-13
1.1.8 public-key local export rsa 1-15
1.1.9 public-key peer 1-17
1.1.10 public-key peer import sshkey 1-18

# 1 公钥管理

## 1.1 公钥管理配置命令

### 1.1.1 display public-key local public

**display public-key local public** 命令用来显示本地非对称密钥对中的公钥信息。

【命令】

**display public-key local** { **dsa** | **ecdsa** | **rsa** } **public** [ **name** *key-name* ]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

**dsa**：显示本地 DSA 密钥对中的公钥信息。

**ecdsa**：显示本地 ECDSA 密钥对中的公钥信息。

**rsa**：显示本地 RSA 密钥对中的公钥信息。

**name** *key-name*：显示指定的本地非对称密钥对的公钥信息。*key-name* 为本地非对称密钥对的名称，为 1～64 个字符的字符串，不区分大小写，字符串中可以包含字母、数字及“-”。如果不指定本参数，则显示指定类型的所有本地非对称密钥对的公钥信息。

【使用指导】

如果通过手工配置方式将本地的主机公钥保存到远端设备上，则需要事先在本地设备上执行本命令显示主机公钥信息，并记录该信息。

对于默认名称的密钥对，不能通过指定 **name** *key-name* 参数显示；显示指定类型的所有本地非对称密钥对时会显示默认名称的密钥对。

【举例】

# 显示所有本地 RSA 密钥对中的公钥信息。

```
<Sysname> display public-key local rsa public

=============================================
Key name: hostkey (default)
Key type: RSA
Time when key pair created: 15:40:48 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
   667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
   C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
   FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
```

```
   2DA4C04EF5AE0835090203010001
=============================================
Key name: serverkey (default)
Key type: RSA
Time when key pair created: 15:40:48 2011/05/12
Key code:
   307C300D06092A864886F70D0101010500036B003068026100CAB4CACCA16442AD5F453442
   762F03897E0D494FEDE69224F5C051A441D290976733A278C9F0C0F5A198E66143EAB54A64
   DB608269CAE844B1E7CC64AD7E808972E7CF887F3B657F056E7930FC84FBF1AD83A01CC47E
   9D85C13413996ECD093B0203010001
=============================================
Key name: rsa1
Key type: RSA
Time when key pair created: 15:42:26 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DEBC46F217DDF11D
   426E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
   1A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
   9A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03
   92D8C6D940890BF4290203010001
```

# 显示所有本地 DSA 密钥对中的公钥信息。

```
<Sysname> display public-key local dsa public

=============================================
Key name: dsakey (default)
Key type: DSA
Time when key pair created: 15:41:37 2011/05/12
Key code:
   308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF038184000281804191 2CE34D12BCD2157E7AB1C2F03B3EF395
   100F3DB4A9E2FDFE860C1BD663D676438F7DA40A9406D61CA9079AF13E330489F1C76785DE
   52DA649AC8BC04B6D39CD7C52CD0A14F75F7491A91D31D6AC22340B5981B27A915CDEC4F09
   887E541EC1E5302D500F68E7AC29A084463C60F9EE266985A502FC92193E1CF4D265C4BA
=============================================
Key name: dsa1
Key type: DSA
Time when key pair created: 15:35:42 2011/05/12
Key code:
   308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
```

```
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF0381850002818100A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
   3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
   0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
   15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

# 显示所有本地 ECDSA 密钥对中的公钥信息。

```
<Sysname> display public-key local ecdsa public

=============================================
Key name: ecdsakey (default)
Key type: ECDSA
Time when key pair created: 15:42:04 2011/05/12
Key code:
   3049301306072A8648CE3D020106082A8648CE3D03010103320004C10CF7CE42193F7FC2AF
   68F5DC877835A43009DB6135558A7FB8316C361B0690B4FD84A14C0779C76DD6145BF9362B
   1D
=============================================
Key name: ecdsa1
Key type: ECDSA
Time when key pair created: 15:43:33 2011/05/12
Key code:
   3049301306072A8648CE3D020106082A8648CE3D03010103320004A1FB84D92315B8DB72D1
   AE672C7CFA5135D5F5B02377F2F092F182EC83B5819795BC94CCBD3EBA7D4F0F2B2EB20C58
   4D
```

# 显示名称为 rsa1 的本地 RSA 密钥对中的公钥信息。

```
<Sysname> display public-key local rsa public name rsa1

=============================================
Key name: rsa1
Key type: RSA
Time when key pair created: 15:42:26 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DEBC46F217DDF11D
   426E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
   1A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
   9A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03
   92D8C6D940890BF4290203010001
```

# 显示名称为 dsa1 的本地 DSA 密钥对中的公钥信息。

```
<Sysname> display public-key local dsa public name dsa1

=============================================
Key name: dsa1
Key type: DSA
Time when key pair created: 15:35:42 2011/05/12
```

```
Key code:
   308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF0381850002818100A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
   3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
   0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
   15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

# 显示名称为 ecdsa1 的本地 ECDSA 密钥对中的公钥信息。

```
<Sysname> display public-key local ecdsa public name ecdsa1

=============================================
Key name: ecdsa1
Key type: ECDSA
Time when key pair created: 15:43:33 2011/05/12
Key code:
   3049301306072A8648CE3D020106082A8648CE3D03010103320004A1FB84D92315B8DB72D1
   AE672C7CFA5135D5F5B02377F2F092F182EC83B5819795BC94CCBD3EBA7D4F0F2B2EB20C58
   4D
```

表1-1 display public-key local public 命令显示信息描述表

| 字段 | 描述 |
|---|---|
| Key name | 本地非对称密钥对的名称<br>default表示该名称为密钥对的默认名称，即执行**public-key local create**命令没有指定密钥名称时，生成的密钥对的名称<br>• hostkey：RSA 主机密钥对的默认名称<br>• serverkey：RSA 服务器密钥对的默认名称。只有密钥类型为 RSA 时，才会存在服务器密钥对<br>• dsakey：DSA 主机密钥对的默认名称<br>• ecdsakey：ECDSA 主机密钥对的默认名称 |
| Key type | 密钥类型，取值包括：<br>• RSA：密钥类型为 RSA<br>• DSA：密钥类型为 DSA<br>• ECDSA：密钥类型为 ECDSA |
| Time when key pair created | 本地非对称密钥对产生的时间 |
| Key code | 本地非对称密钥对的公钥数据 |

## 【相关命令】

- **public-key local create**

### 1.1.2 display public-key peer

**display public-key peer** 命令用来显示保存在本地的远端主机的公钥信息。

【命令】

**display public-key peer** [ **brief** | **name** *publickey-name* ]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

**brief**：显示保存在本地的所有远端主机公钥的简要信息。

**name** *publickey-name*：显示保存在本地的指定远端主机公钥的详细信息，*publickey-name* 为远端主机公钥的名称，为 1～64 个字符的字符串，区分大小写。

【使用指导】

如果没有指定任何参数，则显示所有保存在本地的远端主机公钥的详细信息。

可以通过 **public-key peer** 命令或 **public-key peer import sshkey** 命令将远端主机的公钥配置到本地。

【举例】

# 显示保存在本地的公钥名称为 idrsa 的远端主机公钥的详细信息。

```
<Sysname> display public-key peer name idrsa

=============================================
Key name: idrsa
Key type: RSA
Key modulus: 1024
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100C5971581A78B5388
   B3C9063EC6B53D395A6704D9752B6F9B7B1F734EEB5DD509F0B050662C46FFB8D27F797E37
   918F6270C5793F1FC63638970A0E4D51A3CEF7CFF6E92BFAFD73F530E0BDE27056E81F2525
   6D0883836FD8E68031B2C272FE2EA75C87734A7B8F85B8EBEB3BD51CC26916AF3B3FDC32C3
   42C142D41BB4884FEB0203010001
```

表1-2 display public-key peer name 命令显示信息描述表

| 字段 | 描述 |
|---|---|
| Key name | 远端主机公钥的名称 |
| Key type | 密钥类型，取值包括RSA、DSA和ECDSA |
| Key modulus | 密钥模数的长度，单位为比特 |
| Key code | 公钥数据 |

# 显示保存在本地的所有远端主机公钥的简要信息。

```
<Sysname> display public-key peer brief
Type  Modulus  Name
--------------------------
RSA   1024    idrsa
DSA   1024    10.1.1.1
```

表1-3 display public-key peer brief 命令显示信息描述表

| 字段 | 描述 |
|---|---|
| Type | 密钥类型，取值包括RSA、DSA和ECDSA |
| Modulus | 密钥模数的长度，单位为比特 |
| Name | 远端主机公钥的名称 |

【相关命令】

- **public-key peer**
- **public-key peer import sshkey**

## 1.1.3 peer-public-key end

**peer-public-key end** 命令用来从公钥视图退回到系统视图，并保存用户输入的公钥。

【命令】

**peer-public-key end**

【视图】

公钥视图

【缺省用户角色】

network-admin

【使用指导】

本命令用于通过手工配置方式将远端主机的公钥保存到本地设备上。手工配置方式是指：

(1) 执行 **public-key peer** 命令进入公钥视图。

(2) 在公钥视图手工输入远端主机的公钥。

(3) 执行 **peer-public-key end** 命令退出公钥视图，并保存输入的公钥。

输入的公钥数据必须满足一定的格式要求。在保存公钥之前，设备会进行公钥合法性的检测：

- 如果用户配置的公钥字符串不满足格式要求，那么将会显示相关提示信息，用户配置的公钥将被丢弃，本次配置失败；
- 如果用户配置的公钥字符串合法，例如输入的公钥数据为通过 **display public-key local public** 命令显示的公钥，则保存该公钥。

【举例】

# 退出公钥视图，并保存用户输入的公钥。

```
<Sysname> system-view
[Sysname] public-key peer key1
```

```
Enter public key view. Return to system view with "peer-public-key end" command.
[Sysname-pkey-public-key-key1]30819F300D06092A864886F70D010101050003818D0030818902818100
C0EC8014F82515F6335A0A
[Sysname-pkey-public-key-key1]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C29481B77E719
D1643135877E13B1C531B4
[Sysname-pkey-public-key-key1]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B854E2371D5B952
ADF6B80EB5F52698FCF3D6
[Sysname-pkey-public-key-key1]1F0C2EAAD9813ECB16C5C7DC09812D4EE3E9A0B074276FFD4AF2050BD4
A9B1DDE675AC30CB020301
[Sysname-pkey-public-key-key1]0001
[Sysname-pkey-public-key-key1] peer-public-key end
[Sysname]
```

【相关命令】

- **display public-key local public**
- **display public-key peer**
- **public-key peer**

### 1.1.4 public-key local create

**public-key local create** 命令用来生成本地非对称密钥对。

【命令】

**public-key local create** { **dsa** | **ecdsa** [ **secp192r1** | **secp256r1** | **secp384r1** | **secp521r1** ] | **rsa** } [ **name** *key-name* ]

【缺省情况】

不存在本地非对称密钥对。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

**dsa**：本地密钥对类型为 DSA。

**ecdsa**：本地密钥对类型为 ECDSA。

- **secp192r1**：采用名称为 secp192r1 的椭圆曲线生成本地 ECDSA 密钥对，密钥长度为 192 比特。
- **secp256r1**：采用名称为 secp256r1 的椭圆曲线生成本地 ECDSA 密钥对，密钥长度为 256 比特。
- **secp384r1**：采用名称为 secp384r1 的椭圆曲线生成本地 ECDSA 密钥对，密钥长度为 384 比特。
- **secp521r1**：采用名称为 secp521r1 的椭圆曲线生成本地 ECDSA 密钥对，密钥长度为 521 比特。

如果不指定以上任一种密钥对算法参数，则采用名称为 secp192r1 的椭圆曲线生成本地 ECDSA 密钥对，密钥长度为 192 比特。

**rsa**：本地密钥对类型为 RSA。

**name** *key-name*：生成指定名称的本地非对称密钥对。*key-name* 为本地非对称密钥对的名称，为 1～64 个字符的字符串，不区分大小写，字符串中只能包含字母、数字及“-”。如果不指定本参数，则生成的 RSA 主机密钥对的默认名称为 hostkey，RSA 服务器密钥对的默认名称为 serverkey，DSA 密钥对的默认名称为 dsakey，ECDSA 密钥对的默认名称为 ecdsakey。

【使用指导】

创建RSA和DSA密钥对时，设备会提示用户输入密钥模数的长度。密钥模数越长，安全性越好，但是生成密钥的时间越长。创建ECDSA密钥对时，可使用不同密钥长度的椭圆曲线，密钥越长，安全性越好，但是生成密钥的时间越长。关于密钥模数长度的配置限制和注意事项请参见 表 1-4。

生成密钥对时，如果不指定密钥对名称，系统会以缺省名称命名密钥对，并把该密钥对标记为默认（default）。

用户可以使用缺省的密钥对名称创建其他密钥对，但系统不会把该密钥对标记为默认（default）。

非默认名称密钥对的密钥类型和名称不能完全相同，否则需要用户确认是否覆盖原有的密钥对。不同类型的密钥对，名称可以相同。

执行此命令后，生成的密钥对将保存在设备中，设备重启后密钥不会丢失。

表1-4 不同类型密钥对对比

| 密钥对类型 | 生成的密钥对 | 密钥模数长度 |
|---|---|---|
| RSA | • 不指定密钥对名称时，将同时生成两个密钥对服务器密钥对和主机密钥对<br>• 指定密钥对名称时，只生成一个主机密钥对<br>说明<br>目前，只有 SSH1.5 中应用了 RSA 服务器密钥对 | 长度取值范围为512～2048比特，缺省值为1024比特，建议密钥模数的长度大于或等于768比特 |
| DSA | 只生成一个主机密钥对 | 长度取值范围为512～2048比特，缺省值为1024比特，建议密钥模数的长度大于或等于768比特 |
| ECDSA | 只生成一个主机密钥对 | 长度取值为192、256、384或521比特 |

【举例】

# 生成默认名称的本地 RSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...++++++
```

```
.++++++
..++++++++
....++++++++
Create the key pair successfully.
```

# 生成默认名称的本地 DSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+..+.............
.......+.........+............+............+...+.....+.............+..+...
...+................+.........+...+....+.......+.....+...........+........+.
.....................+........+.........+............+.....+...+.........
.............+........+.........+..........+........+....+................
.....++++++++++++++++++++++++++++++++++++++++++++++++++*
Create the key pair successfully.
```

# 生成默认名称的本地 ECDSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local create ecdsa
Generating Keys...
Create the key pair successfully.
```

# 生成名称为 rsa1 的本地 RSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local create rsa name rsa1
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...++++++
.............................++++++
Create the key pair successfully.
```

# 生成名称为 dsa1 的本地 DSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local create dsa name dsa1
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+..+.............
.......+.........+............+............+...+.....+.............+..+...
```

```
...+.................+.........+...+....+.......+.....+...........+.........+.
.......................+........+.........+.............+.....+...+..........
..............+.........+.........+..........+........+....+..................
.....++++++++++++++++++++++++++++++++++++++++++++++++++++++++*
Create the key pair successfully.
```

# 生成名称为 ecdsa1 的本地 ECDSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local create ecdsa name ecdsa1
Generating Keys...
Create the key pair successfully.
```

【相关命令】

- **display public-key local public**
- **public-key local destroy**

### 1.1.5 public-key local destroy

**public-key local destroy** 命令用来销毁本地非对称密钥对。

【命令】

**public-key local destroy** { **dsa** | **ecdsa** | **rsa** } [ **name** *key-name* ]

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

**dsa**：本地密钥对类型为 DSA。

**ecdsa**：本地密钥对类型为 ECDSA。

**rsa**：本地密钥对类型为 RSA。

**name** *key-name*：销毁指定名称的本地非对称密钥对。*key-name* 为本地非对称密钥对名称，为 1～64 个字符的字符串，不区分大小写，字符串中可以包含字母、数字及“-”。如果不指定本参数，则销毁指定类型默认名称的本地非对称密钥对。

【使用指导】

在如下几种情况下，建议用户销毁旧的非对称密钥对，并生成新的密钥对：

- 本地设备的私钥泄露。这种情况下，非法用户可能会冒充本地设备访问网络。
- 保存密钥对的存储设备出现故障，导致设备上没有公钥对应的私钥，无法再利用旧的非对称密钥对进行加解密和数字签名。
- 密钥对使用了较长时间，可能存在密钥泄露或破译的风险。
- 本地证书到达有效期，需要删除对应的本地密钥对。本地证书的详细介绍，请参见“安全配置指导”中的“PKI”。

【举例】

# 销毁默认名称的本地 RSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local destroy rsa
Confirm to destroy the key pair? [Y/N]:y
```

# 销毁默认名称的本地 DSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local destroy dsa
Confirm to destroy the key pair? [Y/N] :y
```

# 销毁默认名称的本地 ECDSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local destroy ecdsa
Confirm to destroy the key pair? [Y/N]:y
```

# 销毁名称为 rsa1 的本地 RSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local destroy rsa name rsa1
Confirm to destroy the key pair? [Y/N]:y
```

# 销毁名称为 dsa1 的本地 DSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local destroy dsa name dsa1
Confirm to destroy the key pair? [Y/N] :y
```

# 销毁名称为 ecdsa1 的本地 ECDSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local destroy ecdsa name ecdsa1
Confirm to destroy the key pair? [Y/N]:y
```

**【相关命令】**

- **public-key local create**

### 1.1.6 public-key local export dsa

**public-key local export dsa** 命令用来根据指定格式显示本地 DSA 主机公钥或将其导出到指定文件。

**【命令】**

**public-key local export dsa** [ **name** *key-name* ] { **openssh** | **ssh2** } [ *filename* ]

**【视图】**

系统视图

**【缺省用户角色】**

network-admin

**【参数】**

**name** *key-name*：显示或导出指定本地 DSA 密钥对的主机公钥。*key-name* 为本地密钥对的名称，为 1～64 个字符的字符串，不区分大小写，字符串中可以包含字母、数字及“-”。如果不指定本参数，则显示或导出默认名称的本地 DSA 密钥对的主机公钥。

**openssh**：主机公钥格式为 OpenSSH。

**ssh2**：主机公钥格式为 SSH2.0。

*filename*：指定存储导出公钥的文件的名称，不区分大小写，取值不能为“hostkey”、“serverkey”、“dsakey”、“ecdsakey”，不能全部为“.”，并且第一个字符不能为“/”，不能包含字符串“./”和“../”。文件名长度取值范围为 1~128。文件名的详细介绍，请参见“基础配置指导”中的“文件系统管理”。如果不指定本参数，则按照指定格式显示本地 DSA 主机公钥。

【使用指导】

通过以下操作，采用从公钥文件中导入的方式将本地的主机公钥保存到远端设备上：

(1) 通过以下任一方法将导出的公钥保存到文件中：

- 在本地设备上执行 **public-key local export** 命令按照指定格式显示本地主机公钥（执行命令时不指定 *filename* 参数），再通过粘贴复制方式将显示的主机公钥保存到文件中。
- 在本地设备上执行 **public-key local export** 命令按照指定格式将本地主机公钥导出到指定文件（执行命令时指定 *filename* 参数）。需要注意的是，不能将主机公钥导出到工作路径 pkey 目录以及 pkey 的子目录中。

(2) 将所获得的证书文件通过 FTP 的二进制模式或 TFTP 上传到远端主机。有关 FTP 和 TFTP 的详细使用请参见“基础配置指导”中的“FTP 和 TFTP”。

(3) 在远端主机上，执行 **public-key peer import sshkey** 命令将主机公钥保存到本地上。

SSH2.0 和 OpenSSH 是两种不同类型的公钥格式，用户需要根据服务器端支持的对端公钥格式，来选择导出的主机公钥格式。

【举例】

# 以 OpenSSH 格式导出默认名称的本地 DSA 密钥对的主机公钥，存储导出公钥的文件名为 key.pub。

```
<Sysname> system-view
[Sysname] public-key local export dsa openssh key.pub
```

# 以 SSH2.0 格式显示默认名称的本地 DSA 密钥对的主机公钥。

```
<Sysname> system-view
[Sysname] public-key local export dsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-2011/05/12"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3B7b
0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbzWCFLFq
L6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN
/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2B
cdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACAQZEs400SvNIVfnqxwvA7PvOVEA89tKni
/f6GDBvWY9Z2Q499pAqUBtYcqQea8T4zBInxx2eF3lLaZJrIvAS205zXxSzQoU9190kakdMdasIjQLWYGyepFc3s
TwmIflQeweUwLVAPaOesKaCERjxg+e4maYWlAvySGT4c9NJlxLo=
---- END SSH2 PUBLIC KEY ----
```

# 以 OpenSSH 格式显示默认名称的本地 DSA 密钥对的主机公钥。

```
<Sysname> system-view
[Sysname] public-key local export dsa openssh
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3B7b
0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbzWCFLFq
L6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN
/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2B
cdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACAQZEs400SvNIVfnqxwvA7PvOVEA89tKni
/f6GDBvWY9Z2Q499pAqUBtYcqQea8T4zBInxx2eF3lLaZJrIvAS205zXxSzQoU9190kakdMdasIjQLWYGyepFc3s
TwmIflQeweUwLVAPaOesKaCERjxg+e4maYWlAvySGT4c9NJlxLo= dsa-key
```

# 以 OpenSSH 格式导出名称为 dsa1 的本地 DSA 密钥对的主机公钥，文件名为 dsa1.pub。

```
<Sysname> system-view
[Sysname] public-key local export dsa name dsa1 openssh dsa1.pub
```

# 以 SSH2.0 格式显示名称为 dsa1 的本地 DSA 密钥对的主机公钥。

```
<Sysname> system-view
[Sysname] public-key local export dsa name dsa1 ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-2011/05/12"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3B7b
0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbzWCFLFq
L6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN
/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2B
cdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACBAKHkVsjaKtG7g7G98qGmtaboNkK0YEAk
Rdp+QDZxX0aPdmVeEU1GC3ES9XFD7gIK70pb+tB7dA+8scZNqKK85hkoNCFEXux3088NEYZullatZRH0km+DdpZ7
CrcV+ft7UUvBF0FV3W4HOx/LOidJ5sX+qBAD4WcpSX0OrZEF4+dq
---- END SSH2 PUBLIC KEY ----
```

# 以 OpenSSH 格式显示名称为 dsa1 的本地 DSA 密钥对的主机公钥。

```
<Sysname> system-view
[Sysname] public-key local export dsa name dsa1 openssh
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3B7b
0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbzWCFLFq
L6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN
/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2B
cdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACBAKHkVsjaKtG7g7G98qGmtaboNkK0YEAk
Rdp+QDZxX0aPdmVeEU1GC3ES9XFD7gIK70pb+tB7dA+8scZNqKK85hkoNCFEXux3088NEYZullatZRH0km+DdpZ7
CrcV+ft7UUvBF0FV3W4HOx/LOidJ5sX+qBAD4WcpSX0OrZEF4+dq dsa-key
```

【相关命令】

- **public-key local create**
- **public-key peer import sshkey**

## 1.1.7 public-key local export ecdsa

**public-key local export ecdsa** 命令用来根据指定格式显示本地 ECDSA 主机公钥或将其导出到指定文件。

【命令】

**public-key local export ecdsa** [ **name** *key-keyname* ] { **openssh** | **ssh2** } [ *filename* ]

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

**name** *key-name*：显示或导出指定本地 ECDSA 密钥对的主机公钥。*key-name* 为本地密钥对的名称，为 1～64 个字符的字符串，不区分大小写，字符串中可以包含字母、数字及“-”。如果不指定本参数，则显示或导出默认名称的本地 ECDSA 密钥对的主机公钥。

**openssh**：主机公钥格式为 OpenSSH。

**ssh2**：主机公钥格式为 SSH2.0。

*filename*：指定存储导出公钥的文件的名称，不区分大小写，取值不能为“hostkey”、“serverkey”、“dsakey”、“ecdsakey”，不能全部为“.”，并且第一个字符不能为“/”，不能包含字符串“./”和“../”。文件名长度取值范围为 1~128。文件名的详细介绍，请参见“基础配置指导”中的“文件系统管理”。如果不指定本参数，则按照指定格式显示本地 ECDSA 主机公钥。

【使用指导】

通过以下操作，采用从公钥文件中导入的方式将本地的主机公钥保存到远端设备上：

(1) 通过以下任一方法将导出的公钥保存到文件中：

- 在本地设备上执行 **public-key local export** 命令按照指定格式显示本地主机公钥（执行命令时不指定 *filename* 参数），再通过粘贴复制方式将显示的主机公钥保存到文件中。
- 在本地设备上执行 **public-key local export** 命令按照指定格式将本地主机公钥导出到指定文件（执行命令时指定 *filename* 参数）。需要注意的是，不能将主机公钥导出到工作路径 pkey 目录以及 pkey 的子目录中。

(2) 将所获得的证书文件通过 FTP 的二进制模式或 TFTP 上传到远端主机。有关 FTP 和 TFTP 的详细使用请参见“基础配置指导”中的“FTP 和 TFTP”。

(3) 在远端主机上，执行 **public-key peer import sshkey** 命令将主机公钥保存到本地。

SSH2.0 和 OpenSSH 是两种不同类型的公钥格式，用户需要根据服务器端支持的对端公钥格式，来选择导出的主机公钥格式。

目前，只支持导出椭圆曲线为 **secp256r1** 的 ECDSA 主机公钥。

【举例】

# 以 OpenSSH 格式导出本地 ECDSA 主机公钥，存储导出公钥的文件名为 key.pub。

```
<Sysname> system-view
[Sysname] public-key local export ecdsa openssh key.pub
```

# 以 SSH2.0 格式显示本地 ECDSA 主机公钥。

```
<Sysname> system-view
[Sysname] public-key local export ecdsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "ecdsa-sha2-nistp256-2014/07/06"
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBREw5tkARpbV+sYArt/xcW+UJEAevx7OckT
tTLPBiLP5bWkSdKbvo+3oHRuIyZqmNTIcxuBjuBap+pHc919C58=
---- END SSH2 PUBLIC KEY ----
```

# 以 OpenSSH 格式显示本地 ECDSA 主机公钥。

```
<Sysname> system-view
[Sysname] public-key local export ecdsa openssh
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBREw5tkARpbV+sYArt/xcW+UJEAevx7OckT
tTLPBiLP5bWkSdKbvo+3oHRuIyZqmNTIcxuBjuBap+pHc919C58=
```

ecdsa-key

【相关命令】

**public-key local create**

**public-key peer import sshkey**

### 1.1.8 public-key local export rsa

**public-key local export rsa** 命令用来根据指定格式显示本地 RSA 主机公钥或将其导出到指定文件。

【命令】

**public-key local export rsa** [ **name** *key-name* ] { **openssh** | **ssh1** | **ssh2** } [ *filename* ]

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

**name** *key-name*：显示或导出指定本地 RSA 密钥对的主机公钥。*key-name* 为本地密钥对的名称，为 1～64 个字符的字符串，不区分大小写，字符串中可以包含字母、数字及“-”。如果不指定本参数，则显示或导出默认名称的本地 RSA 密钥对的主机公钥。

**openssh**：主机公钥格式为 OpenSSH。

**ssh1**：主机公钥格式为 SSH1.5。

**ssh2**：主机公钥格式为 SSH2.0。

*filename*：指定存储导出公钥的文件的名称，不区分大小写，取值不能为“hostkey”、“serverkey”、“dsakey”、“ecdsakey”，不能全部为“.”，并且第一个字符不能为“/”，不能包含字符串“./”和“../”。文件名长度取值范围为 1~128。文件名的详细介绍，请参见“基础配置指导”中的“文件系统管理”。如果不指定本参数，则按照指定格式显示本地 RSA 主机公钥。

【使用指导】

通过以下操作，采用从公钥文件中导入的方式将本地的主机公钥保存到远端设备上：

(1) 通过以下任一方法将导出的公钥保存到文件中：

- 在本地设备上执行 **public-key local export** 命令按照指定格式显示本地主机公钥（执行命令时不指定 *filename* 参数），再通过粘贴复制方式将显示的主机公钥保存到文件中。
- 在本地设备上执行 **public-key local export** 命令按照指定格式将本地主机公钥导出到指定文件（执行命令时指定 *filename* 参数）。需要注意的是，不能将主机公钥导出到工作路径 pkey 目录以及 pkey 的子目录中。

(2) 将所获得的证书文件通过 FTP 的二进制模式或 TFTP 上传到远端主机。有关 FTP 和 TFTP 的详细使用请参见“基础配置指导”中的“FTP 和 TFTP”。

(3) 在远端主机上，执行 **public-key peer import sshkey** 命令将主机公钥保存到本地。

SSH1.5、SSH2.0 和 OpenSSH 是三种不同类型的公钥格式，用户需要根据服务器端支持的对端公钥格式，来选择导出的主机公钥格式。

【举例】

# 以 OpenSSH 格式导出默认名称的本地 RSA 密钥对的主机公钥，存储导出公钥的文件名为 key.pub。

```
<Sysname> system-view
[Sysname] public-key local export rsa openssh key.pub
```

# 以 SSH2.0 格式显示默认名称的本地 RSA 密钥对的主机公钥。

```
<Sysname> system-view
[Sysname] public-key local export rsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-2011/05/12"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDapKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGMrSfddq/bYcb
gM7Buit1AgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/aj1k3rM+XOvyvPJilneKJqhPT0xdv4tlas
+mLNloY0dImbwS2kwE71rgg1CQ==
---- END SSH2 PUBLIC KEY ----
```

# 以 OpenSSH 格式显示默认名称的本地 RSA 密钥对的主机公钥。

```
<Sysname> system-view
[Sysname] public-key local export rsa openssh
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDapKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGMrSfddq/bYcb
gM7Buit1AgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/aj1k3rM+XOvyvPJilneKJqhPT0xdv4tlas
+mLNloY0dImbwS2kwE71rgg1CQ== rsa-key
```

# 以 OpenSSH 格式导出名称为 rsa1 的本地 RSA 密钥对的主机公钥，文件名为 rsa1.pub。

```
<Sysname> system-view
[Sysname] public-key local export rsa name rsa1 openssh rsa1.pub
```

# 以 SSH2.0 格式显示名称为 rsa1 的本地 RSA 密钥对的主机公钥。

```
<Sysname> system-view
[Sysname] public-key local export rsa name rsa1 ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-2011/05/12"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDevEbyF93xHUJucJWqRc1r8fhzQ9lSVprCI6ATZeDYyR1J00fBQ8XY+q2o
lqoagn5YDyUC8ZJvUhlyMOHeORpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05t8mCLVaupbfCzP8ba8UkrU
mMO4fUvW6zavA5LYxtlAiQv0KQ==
---- END SSH2 PUBLIC KEY ----
```

# 以 OpenSSH 格式显示名称为 rsa1 的本地 RSA 密钥对的主机公钥。

```
<Sysname> system-view
[Sysname] public-key local export rsa name rsa1 openssh
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDevEbyF93xHUJucJWqRc1r8fhzQ9lSVprCI6ATZeDYyR1J00fBQ8XY+q2o
lqoagn5YDyUC8ZJvUhlyMOHeORpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05t8mCLVaupbfCzP8ba8UkrU
mMO4fUvW6zavA5LYxtlAiQv0KQ== rsa-key
```

【相关命令】

- **public-key local create**
- **public-key peer import sshkey**

### 1.1.9 public-key peer

**public-key peer** 命令用来指定远端主机公钥的名称，并进入公钥视图。如果指定的远端主机公钥名称已经存在，则直接接进入该公钥视图。

**undo public-key peer** 命令用来删除指定的远端主机公钥。

【命令】

**public-key peer** *keyname*

**undo public-key peer** *keyname*

【缺省情况】

不存在远端主机公钥。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

*keyname*：远端主机公钥的名称，为 1～64 个字符的字符串，区分大小写。

【使用指导】

进入公钥视图后，可以开始输入公钥数据。在输入公钥数据时，字符之间可以有空格，也可以按回车键继续输入数据。保存公钥数据时，将删除空格和回车符。

通过手工配置方式创建远端主机公钥时，用户需要事先获取并记录远端主机十六进制形式的公钥，并在本地设备上执行以下操作：

(1) 执行本命令进入公钥视图。

(2) 在公钥视图，手工输入远端主机的公钥。

(3) 执行 **peer-public-key end** 命令，保存输入的远端主机公钥，并从公钥视图退回到系统视图。

输入的公钥数据必须满足一定的格式要求。通过 **display public-key local public** 命令显示的公钥可以作为输入的公钥数据。

【举例】

# 指定远端主机公钥名称为 key1，并进入公钥视图。

```
<Sysname> system-view
[Sysname] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
[Sysname-pkey-public-key-key1]
```

【相关命令】

- **display public-key local public**
- **display public-key peer**
- **peer-public-key end**

### 1.1.10 public-key peer import sshkey

**public-key peer import sshkey** 命令用来配置从公钥文件中导入远端主机的公钥。

**undo public-key peer** 命令用来删除指定的远端主机公钥。

【命令】

**public-key peer** *keyname* **import sshkey** *filename*

**undo public-key peer** *keyname*

【缺省情况】

不存在远端主机公钥。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

*keyname*：远端主机公钥的名称，为 1～64 个字符的字符串，区分大小写。

*filename*：指定导入公钥数据的文件名，不区分大小写，取值不能为“hostkey”、“serverkey”、“dsakey”、“ecdsakey”，不能全部为“.”，并且第一个字符不能为“/”，不能包含字符串“./”和“../”。文件名长度取值范围为 1~128。文件名的详细介绍，请参见“基础配置指导”中的“文件系统管理”。

【使用指导】

执行本命令后，系统会对指定公钥文件中的公钥进行格式转换，将其转换为 PKCS 标准编码格式，并将该远端主机的公钥保存到本地设备。

从公钥文件中导入远端主机的公钥前，需要远端主机将其公钥保存到公钥文件中，并将该公钥文件上传到本地设备。例如，在远端主机上执行 **public-key local export** 命令将其公钥导出到公钥文件中，并通过 FTP 或 TFTP，以二进制方式将该公钥文件保存到本地设备。

目前，设备支持的公钥格式为 SSH1.5、SSH2.0 和 OpenSSH。

【举例】

# 配置从公钥文件 key.pub 中导入远端主机的公钥，公钥名称为 key2。

```
<Sysname> system-view
[Sysname] public-key peer key2 import sshkey key.pub
```

【相关命令】

- **display public-key peer**
- **public-key local export dsa**
- **public-key local export ecdsa**
- **public-key local export rsa**